REMARKS

The Applicants have carefully reviewed the Office Action mailed December 24, 2003, and submit the foregoing amendments and following remarks in response thereto. The Applicants canceled claims 1–34 without prejudice to the underlying subject matter, and reserve the right to pursue this subject matter in a continuation application. The Applicants added claims 35–55. Support for new claims 35–55 may be found, generally, within the Specification at Page 10, line 11 to Page 20, line 5 and FIGS. 1–3. The Applicants submit that no new matter has been added to the application. Thus, claims 35–55 are pending.

The Examiner objected to the drawings as failing to comply with 37 C.F.R. § 1.84(p)(5) because they do not include several reference signs mentioned in the Specification, i.e., "200," "300" and "540." The Applicants have amended FIG. 2 to include reference sign "200," amended FIG. 3 to include reference "300" and amended FIG. 5B to include reference sign "540." The Applicants submit that the amended drawings satisfy 37 C.F.R. § 1.84(p)(5) and respectfully request that the Examiner reconsider and withdraw the drawing objection.

The Examiner rejected claim 31 under 35 U.S.C. § 101 as being directed to non–statutory subject matter. The Examiner rejected claims 1–4, 7–10, 16–20, 22–24 and 30–34 under 35 U.S.C. § 102(e) as being anticipated by U.S. Pub. No. 2003/208684 to Camacho et al. ("Camacho"). The Examiner rejected claim 5 under 35 U.S.C. § 103(a) as being unpatentable over Camacho in view of U.S. Pat. No. 6,098,053 to Slater ("Slater"). The Examiner rejected claims 6 and 21 under 35 U.S.C. § 103(a) as being unpatentable over Camacho in view of U.S. Pat. No. 6,047,268 to Bartoli et al. ("Bartoli"). The Examiner rejected claims 11, 14, 15, 25, 28 and 29 under 35 U.S.C. § 103(a) as being unpatentable over Camacho in view of U.S. Pat. No. 6,327,578 to Linehan ("Linehan"). The Examiner rejected claims 12, 13, 26 and 27 under 35 U.S.C. § 103(a) as being unpatentable over Camacho in view of Official Notice. Because the Applicants canceled claims 1–34, these rejections are rendered moot.

The Applicants submit that new claims 35–55 are allowable over the cited references, and respectfully request that the Examiner reconsider and withdraw the pending § 102 and § 103 rejections and find new claims 35–55 allowable over these references.

Claims 35–55 Are Allowable Over the Cited References

Claim 35 is directed to a method for authenticating a payment transaction over a network, and recites, in pertinent part, "storing a public key associated with a public key infrastructure (PKI) key pair in a profile database," "in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, sending a challenge request to the buyer over the network, the challenge request including a message to be digitally signed by the buyer using a private key associated with the PKI key pair," "in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed message, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message" and "if so determined, storing a digitally signed record of the payment transaction in a transaction archive." Claims 42 and 49, directed to a computer readable medium and system, respectively, recite similar subject matter. The Applicants submit that neither Camacho, nor any of the other references cited by the Examiner, disclose these features, either singly or in combination.

Camacho is directed to a distributed personal digital identification (PDI) system that verifies individuals using biometric information prior to approving a transaction or granting access to an online service. Using client system 102, a consumer registers with PDI system 100 by providing a digital code (i.e., a secret word or passphrase) and a biometric template (e.g., fingerprints) collected from the consumer using biometric collection device 102b. PDI system 100 then stores the digital code and biometric profile within a consumer record. *See*, e.g., Col. 8, ¶ 0076 and FIG. 6. After accessing a desired electronic storefront 202 using client 102a and web browser 102c, the consumer submits a purchase transaction request to electronic storefront 202, which redirects the consumer's transaction request data to PDI system 100. If authentication is required, PDI system 100 then requests authentication information from the consumer, including a digital code and current biometric information collected by biometric collection device 102b, verifies the authentication data and then forwards the purchase transaction request to payment service 206, which returns payment approval or disapproval information to electronic storefront 202. *See*, e.g., Col. 5, ¶ 0053 to Col. 6, ¶ 0058 and FIG. 3; Col. 3, ¶ 0034 to Col. 4, ¶ 0042 and FIG. 2; Abstract. The Applicants submit that Camacho fails to disclose many features recited by claims 35, 42 and 49.

Specifically, Camacho teaches that user profile manager 214 may generate a private key and a public key for encrypting and decrypting biometric data as it is collected and returned to PDI system 100 for transaction authentication. Camacho fails to disclose "storing a public key associated with a public key infrastructure (PKI) key pair in a profile database," as recited by claims 35, 42 and 49. Rather, Camacho teaches that the public key is sent to client browser 102c while the private key is stored in a protected directory on PDI system 100, i.e., private key data file 406a in data storage system 220. *See*, e.g., Col. 11, ¶ 0110–11; FIGS. 8C and 9A. Thus, Camacho fails to teach or suggest that the public key may be stored within PDI system 100.

Camacho also teaches that after the consumer's digital code has been authenticated, the consumer's encrypted biometric credentials are compared to those on file for the consumer. "Unlike Digital Code comparisons, however, biometric data is encrypted to protect consumer privacy" (Col. 13, ¶ 0128). Private key file 406a is extracted from data storage system 220 and used to decrypt the biometric information encrypted by the consumer using the public key. PDI system 100 retrieves the stored biometric template for the consumer from "an appropriate biometric database," and then compares the decrypted biometric information to the stored biometric template to determine whether to authorize the transaction. *See*, e.g., Col. 13, ¶ 0129 to Col. 14, ¶ 0135.

Camacho fails to disclose that a "challenge request, including a message to be digitally signed by the buyer using a private key associated with the PKI key pair" may be sent to the buyer in response to an authorization request. Camacho also fails to disclose "determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message" received from the buyer, as recited by claims 35, 42 and 49. Rather, Camacho is *entirely silent* on whether a message may be sent to the consumer, digitally signed using a private key and then returned for authentication. Camacho discloses that the consumer's current biometric information is acquired by biometric collection device 102b, encrypted using a public key and then sent to PDI system 100. Accordingly, Camacho fails to teach or suggest that the consumer may use a private key to encrypt a message received from PDI system 100.

Furthermore, Camacho is *entirely silent* on whether PDI system 100 stores "a digitally signed record of the payment transaction in a transaction archive," as recited by claims 35, 42

and 49. Once the authentication information has been collected from the consumer, PDI system 100 forwards the transaction request to credit payment service 206. Consequently, Camacho fails to teach or suggest that the transaction request can be stored within a database or archive, or whether the stored transaction request may be encrypted using a private key.

Moreover, the Applicants submit that Slater, Bartoli and Linehan also fail to disclose many features recited by claims 35, 42 and 49. Slater is directed to a system for performing online ATM/POS transactions over a public network, and discloses the use of digital certificates to verify purchaser identity and to provide the purchaser public keys to merchant 14 for use in sending an encrypted responses. *See*, e.g., Col. 8, lines 29–51. While Slater discloses that purchaser payment instructions 15 may be digitally signed by purchaser 12, Slater fails to teach or suggest that a "challenge request, including a message to be digitally signed by the buyer using a private key associated with the PKI key pair" may be sent to the buyer in response to an authorization request, "determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message" received from the buyer, or "storing a digitally signed record of the payment transaction in a transaction archive," as recited by claims 35, 42 and 49.

Bartoli is directed to a method for authenticating network transactions using a "cookie" containing both static information (user-identifying information) and dynamic information (transaction-based information). *See*, e.g., Abstract. The Examiner opines that Bartoli discloses that "the record has been digitally signed by the authentication service" (Office Action at Page 6, ¶ 9). While Bartoli discloses that an authorization token, representing the digital signature of the order created by billing system 104, may be sent from billing system 104 to the user's browser, it is the user that "can retain the authorization token for later proof of the order and charges," rather than billing system 104 (Col. 7, lines 35–49). Thus, Bartoli fails to disclose that billing system 104 can store "a digitally signed record of the payment transaction in a transaction archive," as recited by claims 35, 42 and 49. Furthermore, Bartoli fails to teach or suggest that a "challenge request, including a message to be digitally signed by the buyer using a private key associated with the PKI key pair" may be sent to the buyer in response to an authorization request, or "determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message" received from the buyer, as further recited by claims 35, 42 and 49.

Linehan is directed to a "thin" consumer's wallet which adds an issuer gateway to the typical parties involved in an electronic commerce transaction (i.e., the consumer, merchant and issuing bank) in order to move the credit/debit card authorization function from the merchant to the issuer gateway. *See*, e.g., Abstract. However, Linehan is entirely silent on whether a "challenge request, including a message to be digitally signed by the buyer using a private key associated with the PKI key pair" may be sent to the buyer in response to an authorization request. Linehan also fails to disclose "determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed message" received from the buyer, or "storing a digitally signed record of the payment transaction in a transaction archive," as recited by claims 35, 42 and 49.

Accordingly, the Applicants submit that claims 35, 42 and 49 are allowable over the cited references. The Applicants further submit that claims 36–41, depending from claim 35, claims 43–48, depending from claim 42 and claims 50–55, depending from claim 49, are also allowable, at least for the reasons discussed above. The Applicants respectfully request that the Examiner find new claims 35–55 allowable over the cited references, and issue a Notice to that effect.

CONCLUSION

In view of the remarks submitted above, the Applicants respectfully submit that the present case is in condition for allowance. A Notice to that effect would be greatly appreciated.

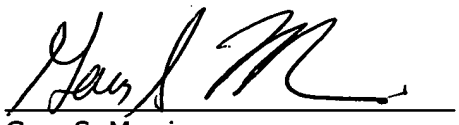
The Examiner is invited to contact the undersigned at (202) 220-4250 to discuss any matter concerning this application.

The Office is authorized to charge any additional fees or credit any overpayments under 37 C.F.R. § 1.16 or § 1.17 to Deposit Account No. 11-0600.

Respectfully submitted,

KENYON & KENYON

April 26, 2004



Gary S. Morris
Registration No. 40,735

1500 K Street, N.W.
Washington, D.C. 20005
(202) 220-4200 (phone)
(202) 220-4201 (fax)